VALTIOVARAINMINISTERIÖ

# Hankkeen tieto-turva-ohje

9/2008 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

# Hankkeen tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä 9/2008 VAHTI


Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Anitta Heiskanen /VM-julkaisutiimi

ISSN 1455-2566
ISBN 978-951-804-895-7 (nid)
ISBN 978-951-804-896-4 (pdf)
Helsinki 2008

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 54/01/2008

OHJE
4.12.2008

Ministeriöille, virastoille ja laitoksille

# HANKKEEN TIETOTURVAOHJE

Valtiovarainministeriön antaman tietoturvaohjeen (VAHTI 9/2008) on tarkoitus parantaa hankkeiden tietoturvallisuutta ja tukea hankkeita niiden elinkaaren aikana tietoturvallisuuden hallinnassa.

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on ohjannut ohjeen valmistelun ja hyväksynyt ohjeen käytettäväksi hankkeiden tietoturvallisuuden yleisohjeena. Ohje on kirjoitettu erityisesti valtionhallinnon tarpeista ja se soveltuu pääosin myös muille organisaatioille.

Hankkeen tietoturvallisuus on ohjeessa kuvattu kokonaisuutena, johon sisältyvät toiminnan prosessit, ihmiset, tietoaineistot ja tietojärjestelmät. Valtionhallinnon organisaatioissa hankkeiden tietoturvallisuudesta tulee huolehtia laaja-alaisesti siten, että se kattaa hankkeen elinkaaren kaikki vaiheet ja tietoturvallisuuden osa-alueet.

Ohjeessa painotetaan hankejohtamisen, hankevetäjän ja muiden toimijoiden vastuiden sekä tietoturvallisuuden suunnittelun näkökulmia. Hankkeiden johtamisessa tulee varmistaa, että tietoturvallisuuden ja riskienhallinnan taso vastaa asetettuja tavoitteita.

Tietoturvallisuuden varmistaminen alkaa valtion organisaatioissa hankkeen alkuvaiheista ja hankkeen perustamisesta sisältäen muun muassa uhka- ja tietoturvariskiarvion laatimisen, riskienhallinnan suunnittelun ja tietoturvallisuutta koskevien toiminnallisten vaatimusten määrittämisen. Tietoturvatoiminnoille tulee hankkeissa varata riittävät resurssit ja osaaminen, joiden mitoitus perustuu hankkeen perustamisvaiheen tietoturvatehtävien tuloksiin.

Hallinto- ja kuntaministeri Mari Kiviniemi

Neuvotteleva virkamies Mikael Kiviniemi
VAHTIn puheenjohtaja

*Liite: HANKKEEN TIETOTURVAOHJE (VAHTI 9/2008)*

# Esipuhe

Tämä ohje toimii hankkeiden tietoturvallisuuden käsikirjana ja esittää tiivistetysti hankkeen tietoturvallisuuden ydinkohdat. Ohje on kirjoitettu valtionhallinnon näkökulmista, mutta se on sovellettavissa myös muissa organisaatioissa.

Ohje painottaa johtamisen, hankevetäjän vastuun ja tietoturvallisuuden suunnittelun näkökulmia. Hankkeen johtamisprosessin osalta tulee varmistaa, että tietoturvallisuuden ja riskienhallinnan taso vastaavat niille asetettuja tavoitteita ja että tietoturvatoiminnoille on varattu riittävät resurssit.

Ohje on valmisteltu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn alaisuudessa ja ohjauksessa. VAHTI päätti ohjeen julkaisemisesta kokouksessaan marraskuussa 2008.

Hankkeen tietoturvaohje julkaistaan VAHTIn verkkosivuilla ja painotuotteena. Ohjeen kaupallinen käyttö ja jäljentäminen ansaitsemistarkoituksessa on kielletty. Muussa hyödyntämisessä tulee tämä ohje mainita lähteenä.

# Lyhyesti VAHTIsta

Valtiovarainministeriö (VM) vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä, kansalaistoiminnassa ja kansainvälisesti. VAHTIn toiminnan tuloksena muun muassa on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut laajan valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta. VAHTI on saanut kolmena perättäisenä vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

# Tiivistelmä

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on tuottanut hallinnon käyttöön tietoturvallisuuden koko kentän kattavan ohje- ja suositusmateriaalin. Tämä ohje toimii hankkeen tietoturvallisuuden käsikirjana esitellen tiivistettynä hankkeen tietoturvallisuuteen liittyvät ydinkohdat.

Ohje pyrkii painottamaan johtamisen näkökulmaa, hankevetäjän vastuuta sekä tietoturvallisuuden suunnitteluun liittyviä toimintoja.

Ohje on kirjoitettu ensisijaisesti valtionhallinnon tarpeet huomioiden, mutta se on pääosin sovellettavissa myös muihin organisaatioihin. Hankkeen tietoturvallisuus on kuvattu kokonaisuutena, joka sisältää toiminnan prosessit ja ihmiset sekä tietoaineistojen ja tietojärjestelmien turvallisuuden ja varmistamisen. Pääkohteina ovat ihmiset, prosessit, tietoaineisto, tietoteknologia ja tietojen käytettävyys. Politiikka, ohjeet, koulutus ja siten syntynyt yhteinen ymmärrys ja toimintatapa ovat organisaation hyvän tietoturvakulttuurin perustekijöitä.

Organisaation sisäinen tietojenkäsittely, tuotanto ja asiakkaiden palveleminen riippuvat kaiken tuotannon taustalla olevien tietojen ja tietojenkäsittelyn luottamuksellisuudesta, eheydestä ja käytettävyydestä - tietoturvallisuudesta. Ilman tietoturvatoimenpiteitä ja etukäteen luotuja vararatkaisuja ei esimerkiksi hankkeen toimintaa voida taata normaalitilanteessa eikä varsinkaan vakavissa häiriötilanteissa.

Hankkeen johtamisprosessin osana tulee varmistaa, että tietoturvallisuuden ja riskienhallinnan taso vastaa sille asetettuja tavoitteita, ja että tietoturvatoiminnoille on varattu riittävät ylläpito- ja kehittämisresurssit.

Ohje tukee organisaatiota hankkeiden tietoturvallisuuden suunnittelussa, toimeenpanossa ja ylläpidossa sekä tarvittavien asiakirjojen laatimisessa.

Ohjeen johdannossa kuvataan tietoturvallisuuden yleisiä periaatteita ja perusteita valtionhallinnon näkökulmasta. Toisessa luvussa käsitellään hankkeen elinkaaren aikana hoidettavia tietoturva-asioita. Kolmannessa luvussa tarkastellaan tietoturvallisuuden osa-alueita hankkeen sisällä. Neljännessä luvussa käsitellään käytettäviä asiakirjoja ja valmiita malleja hankejohtajan käyttöön.

Ohjeen liitteinä on joukko keskeisiä hankkeen tietoturvallisuuden hallintaan liittyviä asiakirjamalleja.

# Sisältö

# 1 Yleistä

## 1.1 Ohjeen käyttö

Tämä ohje on tarkoitettu käytettäväksi erityisesti tietotekniikka- ja tietohallinnon hankkeiden esiselvitys-, määrittely- ja toteutusvaiheissa. Ohjetta voidaan käyttää tapauskohtaisesti soveltaen myös muissa hankkeissa.

Ohje on tarkoitettu erityisesti hankkeisiin, joissa on edustajia useammalta hallinnonalalta ja julkihallinnon organisaatiosta sekä ulkopuolisia asiantuntijoita. Hankkeeseen osallistuvien organisaatioiden hyväksyntä ohjeelle osoittaa, että yhteisistä periaatteista on sovittu työn vaatimassa laajuudessa ja ohjeen perusteella voidaan asettaa vaatimukset ulkopuolisille toimijoille.

Ohje mahdollistaa rajatusti hankkeeseen osallistuvien organisaatioiden välisen luottamussuhteen. Ohje ei täytä kuitenkaan kaikkia valtiohallinnon organisaatioiden tietoturvaperiaatteiden vaatimuksia, joten se ei sellaisenaan välttämättä mahdollista kattavampia luottamussuhteita.

Valtionhallinnossa on muotoutumassa kirjattuja tietoturvapolitiikkoja, joten tässä linjatut asiat ovat ainoastaan tapauskohtaisesti sovellettavissa. Ohjeen periaatteiden mukaan voidaan toimia hankkeissa, joiden tietojen suojausluokka on käyttö rajoitettu tai luottamuksellinen. Turvaluokkien salainen tai erittäin salainen hankkeisiin tulee laatia monilta osin tiukemmat tietoturvakäytännöt.

Tässä ohjeessa tarkastellaan tietoturvallisuutta ja siihen liittyviä ohjeistoja (mm. VAHTI-ohjeisto) hankkeisiin osallistuvien henkilöiden roolien näkökulmasta. Rooleja ovat hanketta ohjaava johto, hankepäällikkö, hankehenkilöstö, hankkeeseen osallistuva valtionhallinnon ja sen ulkopuolinen henkilöstö sekä hanketta ja sen laatua valvova henkilöstö.

Hankkeen ohjausryhmä hyväksyy ohjeen käyttöön. Tällöin keskeiset hankkeeseen osallistuva organisaatiot sitoutuvat hankkeen osalta noudattamaan ohjetta sekä antamaan tarpeelliset tiedot hankkeen käyttöön.

## 1.2 Sidokset muihin ohjeisiin ja normeihin

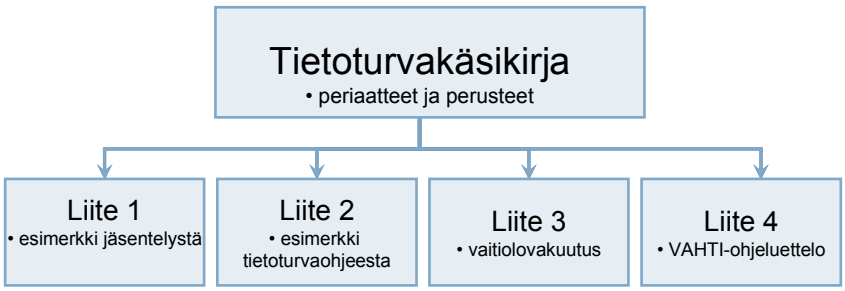
Hankkeen tietoturvaohje perustuu valtiohallinnon normeihin, joita noudatetaan seuraavassa soveltamisjärjestyksessä: tietoturvallisuutta ja yksityisyyden suojaa koskeva lainsäädäntö, muut valtiohallinnon normit, hankkeeseen osallistuvien organisaatioiden tietoturvaohjeet, VAHTI-ohjeisto sekä muut valtiohallinnossa yleisesti noudatetut hyvät käytännöt. Tietoturvaohje valmistellaan yhteistoiminnassa näiden kanssa.

## 1.3 Termit

Ohjeessa noudatetaan Valtiohallinnon tietoturvasanaston (VAHTI 8/2008) mukaisia käsitteitä ja määritelmiä. Poikkeamat tästä mainitaan erikseen.

## 1.4 Ohjeen rakenne ja ylläpito

Ohjeessa on neljä osaa jotka antavat perusteet hankkeen tietoturvallisuuden hallinnalle ja tietoturvakäsikirjan laadintaan. Liitteessä 1 on tietoturvaohjeen jäsentely, jonka pohjalta hankkeen tietoturvaohje voidaan laatia. Liitteessä 2 on esimerkkinä yksittäisen hankkeen tietoturvaohje. Liite 3 on vaitiolovakuutus ja liitteessä 4 on lueteltu voimassaolevat VAHTI-ohjeet. Rakenne on esitetty seuraavassa kuvassa.




Tietoturvakäsikirja on valtionhallinnon VAHTI-ohje ja sen ylläpitämisestä vastaa VAHTI-sihteeristö. Kaikki ohjeen kehittämiseen liittyvät haavainnot tulee toimittaa ylläpitäjälle. Ohje tarkastetaan vähintään kerran VAHTI:n toimintakauden aikana VAHTI-sihteeristössä ja julkaistaan korjattuna tarvittaessa.

## 1.5 Työryhmä

Tämä ohje on laadittu valtionhallinnon tietoturvallisuuden johtoryhmän vuonna 2008 asettamassa ryhmässä, jossa ovat toimineet:

turvallisuusjohtaja Seppo Sundberg, Valtiokonttori, puheenjohtaja

ylitarkastaja Iris Karhuketo, oikeusministeriö

erityisasiantuntija Kalevi Halonen, valtiovarainministeriö

ylitarkastaja Risto Heinonen, tietosuojavaltuutetun toimisto.

Työryhmän sihteerinä on toiminut Sauli Savisalo Digia Oyj:stä.

Valtionhallinnon tietoturvallisuuden johtoryhmä päätti ohjeen julkaisemisesta marraskuussa 2008.

# 2 Tietoturvallisuuden toteuttaminen hankkeiden elinkaaren aikana

## 2.1 Yleistä

Hankkeen tietoturvallisuudella turvataan hankkeessa käsiteltävien tietojen luottamuksellisuus, kiistämättömyys, eheys sekä käytettävyys koko hankkeen ja sen tulosten elinkaaren ajan. Tietoturvallisuudella estetään myös kaupallista syistä tietojen joutuminen asiattomille tahoille (liikesalaisuudet, kaupalliset sopimukset, immateriaaliarvot). Hyvin toteutetulla tietoturvallisuudella edistetään myös hankkeen kustannustehokasta toteutusta.

Hanke voi kattaa yhden osan toiminnan, järjestelmän tai palvelun elinkaarta. Hankkeen tuleekin tietoturvallisuuden kannalta kytkeytyä sitä edeltäneisiin ja seuraaviin vaiheisiin sekä varmistaa erityisesti tietopääoman turvallinen siirtyminen hankkeeseen ja hankkeen loppuessa seuraavaan vaiheeseen.

Hankkeessa käsitellään tietoja useissa vaiheissa ja muodoissa. Niitä voi olla lähdedokumentteina, työssä tuotettuina dokumentteina, suullisessa muodossa työpajoissa ja kokouksissa sekä tulosdokumenteissa. Tyypillistä hankkeille on myös se, että tiedon tuottamiseen ja käsittelyyn osallistuvat useat osapuolet vaihtelevilla tavoilla.

Luottamuksellisuuden turvaamisella varmistetaan, että hankkeella on mahdollisuus saada tietoturvaluokasta riippumatta tarvittavat tiedot käyttöönsä. Turvaamisella varmistetaan myös se, että tiedot eivät joudu hankkeen kautta muiden tietoon vastoin tiedon omistajan tahtoa.

Eheyden turvaamisella varmistetaan muun muassa lähdedokumenttien ja niiden käytön välinen oikea yhteys, dokumenttien versioiden yhdenmukaisuus sekä hyväksyttyjen tulosdokumenttien muuttumattomuus.

Kiistämättömyyden turvaamisella varmistetaan, että hanke on saanut haltuunsa työn kannalta keskeisiä dokumentteja. Sillä varmistetaan myös, että kommentoitavaksi, noudatettavaksi tai muuten käsiteltäväksi toimitetut hankkeen dokumentit on saatettu asianomaisten tahojen käyttöön.

Käytettävyyden turvaamisella varmistetaan työprosessien tehokas läpivienti takaamalla mm. lähde-, työ- ja tulosdokumenttien ja -tietojen saatavuus työn asettamien vaatimusten mukaisesti.

Hankkeen tietoturvallisuuden hallinnassa on kaksi tarkoitusta. Hallinnalla varmistetaan käyttöön saatujen ja tuotettujen tietojen tietoturvallisuus sekä hallinnan avulla voidaan tehdä tietoisia päätöksiä käyttöön hyväksyttävien ja tuotettavien tietojen ja dokumenttien luottamuksellisuuden tasosta. Näiden näkökohtien varmistamiseksi hankkeen tietojen käsittelylle ja turvallisuusluokittelulle määritetään riittävän yksityiskohtaiset periaatteet, jotka kukin osallistuva organisaatio voi rinnastaa omiin mm. asianhallintaan liittyviin periaatteisiinsa.

## 2.2 Vastuut

Hankkeen ohjausryhmä hyväksyy hankkeessa noudatettavat tietoturvallisuuden periaatteet. Tietoturvallisuuden vastuita on myös hankkeeseen liittyvien palvelujen, järjestelmien tai hankintojen valmistelijoilla ja päättäjillä.

Hankepäällikkö vastaa seuraavista asioista:

1. Kokonaisvastuu tietoturvallisuuden hallinnasta, toteuttamisesta sekä valvonnasta auditoinnista hyväksyttyjen periaatteiden mukaisesti.
2. Raportointi tietoturvallisuudesta säännöllisesti ohjausryhmälle.
3. Määrittää esimerkiksi tulosdokumenttien ja käytettävien lähdetietojen tietoturvallisuuden tavoitetason.
4. Määrittää työnaikaiset vastuut, oikeudet ja periaatteet tietoturvaluokan asettamiseen. Tällöin tarkoitetaan tilanteita, joissa useat osapuolet synnyttävät tietoa työprosessissa ja tiedon omistaja on hankepäällikkö.
5. Vastaa työhön osallistuvan henkilöstön ohjeistamisesta, kouluttamisesta sekä valvonnasta. Hankepäällikkö voi vastuuttaa hankehenkilöstöä osaprojektien tai –alueiden tietoturvallisuudesta.

Jokainen hankkeeseen ja sen projekteihin osallistuva henkilö vastaa tietoturvaohjeiden noudattamisesta työssään, havaitsemiensa virheiden poistamisesta sekä erilaisten kehitysehdotusten tekemisestä.

Alaluvut (2.3 – 2.7) käsittelevät tietoturvallisuuden johtamista hankkeen eri vaiheissa (”Mitä tehdään”). Kussakin vaiheessa tulee ottaa huomioon kaikilta tarpeellisilta osiltaan tietoturvallisuuden eri osa-alueet, joiden keskeiset suositukset käytännöiksi on esitetty luvussa 3 (”Miten yleensä”). Hankekohtaisessa

tietoturvasuunnitelmassa esitetään tiivistetysti luvuissa 2 ja 3 luetellut asiat juuri kyseisen hankkeen tapauksessa (”Näin tässä hankkeessa”).

Esimerkki hankekohtaisen tietoturvasuunnitelman jäsentelystä on liitteenä 1 ja yksittäisen hankkeen tietoturvasuunnitelma liitteenä 2.

## 2.3 Hankkeen perustaminen

Hankkeen perustamisen keskeiset tietoturvatehtävät ovat:

1. Uhka- ja tietoturvariskiarvion laatiminen sekä riskien hallinnan suunnittelu.
2. Tietoturvallisuutta koskevien toiminnallisten vaatimusten asettaminen.
3. Hankkeen turvallisuusluokan määrittäminen.
4. Varmistuminen siitä, että tietoturvallisuus tuottaa hankkeen tavoitteisiin oikein suhteutetusti hyötyjä hankkeelle, ei aseta tarpeettomia esteitä tai haittoja tuloksekkaan työn tekemiselle sekä tietoturvallisuutta kehitetään hankeen tarpeiden mukaisesti.
5. Tietoturvakäytäntöjen määrittäminen siten, että jokainen hankkeeseen osallistuva organisaatio sekä tämän edustaja hyväksyy ne ja kykenee suhteuttamaan omat tietoturvaperiaatteensa niihin.
6. Tietoturvaperiaatteiden ja –käytäntöjen hyväksyttäminen ohjausryhmällä.
7. Hankkeen tietoturvaohjeen tuottaminen.
8. Tietoturvaohjeen mukaisten ennakkotoimenpiteiden toteuttaminen ja määriteltyjen edellytysten varmistaminen.
9. Jatkuvan ylläpidon ja valvonnan mekanismin luominen.

Hankepäällikkö vastaa luetelluista toimenpiteistä ennen hankkeen työskentelyn käynnistymistä. Hankepäällikön apuna toimenpiteiden tekemisessä voi olla tietoturva-asiantuntijoita. Suunnitelmia ja periaatteita voidaan joutua tulkitsemaan, täydentämään tai muuttamaan hankkeen aikana. Tällöin muutokset tulee viedä kaikkien yllä kuvattujen vaiheiden kautta läpi.

## 2.4 Ulkopuolisen asiantuntija valinta

Ulkopuolisen asiantuntijan valinnassa keskeiset tietoturvatehtävät ovat:

1. Kilpailuttamisvaiheessa hankkeen turvallisuusperiaatteiden tarkka kuvaaminen, asettaminen keskeisiksi valintakriteereiksi sekä painottaminen arviointikriteeristössä hankkeen turvatason mukaisesti.
2. Varmistuminen siitä, että ulkopuolinen asiantuntija sekä sitoutuu periaatteisiin että kykenee myös täyttämään niiden vaatimukset. Samalla tulee myös varmistua alihankintaketjujen sitoutumisesta ja kyvystä sekä näiden sopimusmenettelyistä omien tukitoimintojensa kanssa.
3. Yritystason turvallisuussopimusten ja auditointien tekeminen tarpeellisessa määrin.
4. Hankehenkilöstön ohjeistaminen toiminnasta ulkopuolisen toimittajan kanssa, mahdollisesti tietoturvaohjeen päivittäminen.
5. Jatkuvan ylläpidon ja valvonnan mekanismin luominen.

Näistä toimenpiteistä vastaavat hankkeen omistaja (kohta 1), hankintahenkilöstö (kohta 2) ja hankepäällikkö (kohdat 3 - 5). Viime kädessä hankepäällikkö vastaa siitä, että ennen ulkopuolisen asiaintuntijan työskentelyn aloittamista kaikki yllä mainitut toimenpiteet on toteutettu. Tästä johtuen hankepäällikön kytkeytyminen työhön jo hankkeen aikaisissa valmisteluvaiheissa on tarkoituksenmukaista. Hankepäällikön työtä helpottaa huomattavasti, mikäli ulkopuolisella asiantuntijalla on nimetty tietoturvallisuuden vastuuhenkilö.

## 2.5 Hankkeen käynnistäminen

Hankkeen käynnistämisen yhteydessä tulee varmistaa, että:

1. Tietoturvasuunnittelu ja -ohjeistus on laadittu, hyväksytty ja sen mukaiset toimenpiteet toteutettu.
2. Hankkeeseen osallistuva henkilöstö on taustatarkistettu sekä koulutettu ja sitoutettu tietoturvallisuuteen.
3. Edellytykset tietoturvaohjeistuksen mukaiseen toimintaan ovat olemassa (mm. asiakirjapohjien, leimojen ja muiden työvälineiden saatavuus) sekä puutteiden korjaamisesta on aikaan sidottu suunnitelma.
4. Hankkeeseen on siirretty tarpeellinen tietoaineisto edeltäviltä vaiheilta ja aineiston tietoturvallisuus on sovitettu hankkeen periaatteisiin.

5. Mahdolliset aiempien vaiheiden toimintatapamallit on sopeutettu hankkeen tietoturvaperiaatteisiin.

Varmistamisesta on vastuussa hankepäällikkö apunaan mahdollisesti organisaation ja ulkopuolisen toimijan tietoturva-asiantuntija. Varmistaminen tulee esitellä ja kirjata tehtynä toimenpiteenä ohjausryhmän pöytäkirjaan.

## 2.6 Hankkeen työskentely

Hankkeen työn aikana tulee:

1. Ylläpitää riskienhallintaa
2. Valvoa ja auditoida työtä tekevien henkilöiden, teknisten järjestelmien sekä tuotosten osalta tietoturvaohjeiden noudattamista.
3. Reagoida tietoturvatapahtumiin ja virheisiin suunnitelman mukaisesti.
4. Ylläpitää tietoturvallisuutta mm. henkilöstön muutoksissa.
5. Raportoida tietoturvallisuudesta ohjausryhmälle.

Hanketyöskentelyn aikana kokonaisvastuu tietoturvallisuudesta on hankepäälliköllä. Tämä voi vastuuttaa hankkeen osavaiheiden tietoturvallisuutta osahankkeista vastaaville, mikäli näillä on tähän todellinen asiantuntemus ja kyky.

## 2.7 Hankkeen valmistuminen

Hankkeen valmistuessa tulee varmistaa, että:

1. Kaikkeen aineistoon ja työmateriaaleihin on merkitty hankepäälikön vahvistama turvallisuusluokitus siten, että materiaali on luovutuskunnossa.
2. Työssä syntynyt säilytettävä aineisto on strukturoidusti ja sovitussa tallennusmuodossa luovutettu.
3. Synnytetty työ- ja välidokumentaatio on hallinnassa.

Hankepäällikkö vastaa hankkeen valmistumiseen liittyvistä tietoturvakysymyksistä. Tietoturvallisuuden hyvä toteutus on hyvin lähellä hankkeen muutoinkin laadukasta toteuttamista.

## 2.8 Hankkeen lopettaminen

Hankkeen lopettamisvaiheessa tulee varmistaa, että:

1. Kaikki hävitettäväksi päätetty sähköinen ja paperidokumentaatio on hävitetty raportoidusti tietoturvaohjeen määrittämällä tavalla.
2. Kaikki taltioitava työ- ja välidokumentaatio on luovutettu ohjausryhmän päättämille tahoille vahvistettu turvallisuusluokitus merkittynä ja materiaali on tarvittaessa kirjattuna haltijoiden diaariin.
3. Hankkeeseen osallistuville on selkeästi kerrottu hankkeen loppumisen jälkeiset vastuut tietoturvallisuudesta ja vastuut seuraaville vaiheille on luovutettu.
4. Hankkeen loppuraporttiin on lisätty keskeiset kohdat tietoturvallisuuden toteuttamisesta ja toteutumisesta.
5. Hankkeen tietoturvaohjeeseen on tehty hankkeen aikana syntyneet parannusehdotukset.

Hankepäällikkö vastaa hankkeen tietoturvakysymyksistä sen lopettamiseen asti. Lopettamiseen liittyvien tietoturvatoimenpiteiden suorittaminen tulee esitellä ja merkitä hankkeen päättämiseen liittyvään ohjausryhmän kokouspöytäkirjaan. Mikäli toimenpiteitä jää suoritettavaksi myöhemmin, näiden vastuut ja suoritusajat tulee myös merkitä kokouspöytäkirjaan. Hankkeen lopettamisvaiheessa varmistetaan myös seuraavien vaiheiden mahdollisimman tehokas ja turvallinen käynnistäminen.

## 2.9 Hankkeen viestintä

Hankepäällikkö vastaa hankkeen viestinnästä sen lopettamiseen asti. Viestintäasiat tulee käsitellä käynnistämisen yhteydessä ja hankkeen kokouksissa.

Viestinnässä varaudutaan erilaisiin tilanteisiin ja varataan hankkeen käyttöön viestinnän asiantuntijoita.

Julkisten hankkeiden osalta jokaisen tehtävänä on levittää aktiivisesti tietoa hankkeen toiminnasta ja tietoturvallisuuden tärkeydestä. Jokaisen tiedotustapahtuman suunnittelun yhteydessä sovitaan tarkemmin, kuka vastaa viestinnästä.

Hankkeen viestinnässä on otettava huomioon tietoturvallisuuteen liittyvät näkökohdat siten, että hankeen tietojen luottamuksellisuus ei vaarannu. Viestintämateriaali tulee merkitä ja käsitellä suojausluokan mukaisesti. Erityisesti sidosryhmäviestinnässä tulee tarvittaessa ottaa tilaisuuteen osallistujilta vaitiolositoumus, jos luokittelu sitä edellyttää.

# 3 Hankkeen tietoturvallisuuden osa-alueet

Poikkihallinnollisissa hankkeissa keskeistä on tunnistaa ja sovittaa yhteen tiedon erilaiset turvallisuusluokitteluperiaatteet sekä niitä vastaavat käsittelysäännöt. Yhteen sovitettu luokittelu, käsittelysäännöt sekä näiden noudattaminen muodostavat työn edellyttämän tietoturvallisuuden ja luottamussuhteen. Hankkeessa tarkastelu voidaan rajoittaa kattamaan vain hankkeen tarvitsemat asiat, mistä johtuen tarkastelua ei voida soveltaa hanketta laajemmin.

Hankkeessa, samoin kuin organisaatioissakin, on tärkeää luoda tietoturvallinen tapa toimia, jota kaikki osallistujat noudattavat.

Tietoturvallisuuden tason oikea määrittely ja johdonmukainen hallinta ovat keskeiset näkökohdat työn onnistumisessa. Liian tiukaksi määritetty tietoturvallisuuden taso johtaa joko työn merkittävään vaikeutumiseen tai tietoturvaohjeen kiertämiseen ja sitä kautta tietoturvariskeihin – yleensä toteutuvat molemmat. Liian matalaksi määritetty tietoturvataso puolestaan nostaa riskitasoa ja estää tarpeellisen tiedon käyttöön saamisen luottamuksen puuttuessa tai aiheuttaa tietoriskin toteutumisen.

## 3.1 Hallinnollinen turvallisuus

### 3.1.1 Hankkeen turvallisuusluokka

Hankkeelle voidaan määrittää turvallisuusluokka tai se voi olla julkinen. Turvallisuusluokkia ovat käyttö rajoitettu, luottamuksellinen, salainen ja erittäin salainen.

Hankkeen turvallisuusluokan määrittämisellä koordinoidaan hankkeen kaikkien osa-alueiden turvallisuusjärjestelyjä siten, että hankkeessa voidaan turvallisesti käsitellä luottamuksellisuudeltaan enintään määritellyn luokan tietoja. Hankkeen turvallisuusluokittelu määräytyy siis luottamuksellisuuden luokituksen mukaan.

Hankkeelle tietoturvallisuuden osa-alueille voidaan myös määrittää eri turvallisuusluokitus ja tietojen suojausluokitusta vastaavat käsittelysäännöt. Hankkeessa käsiteltäviä vaativamman suojaluokan tietoja joko ei käsitellä hankkeessa tai niihin sovelletaan erillisiä tiukempia käsittelysääntöjä.

### 3.1.2 Riskienhallinta

Tietoturvariskien arviointi on keskeinen osa riskianalyysiä. Perusteeksi analyysille on luotava käsitys hankkeessa käsiteltävästä tiedosta, työprosesseista, omasta ja ulkopuolisesta henkilöstöstä ja organisaatioista, toimitiloista, tietoteknisistä ympäristöistä ja palveluista, hankkeen elinkaaresta ja sen kytkeytymisestä aiempiin ja myöhempiin vaiheisiin sekä hankkeen merkityksestä ja kriittisyydestä muulle toiminnalle.

Riskianalyysia ei alkuvaiheessa voida tehdä tarkasti. Suunnittelun edetessä perusteet tarkentuvat, mikä mahdollistaa iteraatiokierroksilla riskianalyysinkin kehittämisen. Riskianalyysiä tulee muutenkin päivittää säännönmukaisesti hankkeen aikana.

Analyysissä tulee arvioida ainakin luottamussuhteen syntymistä ja säilyttämistä, tietojen käyttöön saamista, tietojen varmistamista, käytettävyyttä, kiistämättömyyttä ja eheyttä sekä tietojen luottamuksellisuuden määrittämistä ja takaamista.

Pääosin tietoturvariskeihin on varauduttu normaaleilla erilaisten ohjeiden ja hyvien käytäntöjen mukaisilla perusmenettelyillä. Näiden toimivuutta valvovat palvelujen tuottajat ja toiminnasta vastaavat ilman eri ohjeistusta. Hankepäällikön on kuitenkin syytä varmistautua tästä.

Perusmenettelyjen ulkopuolelle jäävät riskit tulee arvioida sekä niiden todennäköisyyden että vaikutusten näkökulmista. Vaikutuksessa tulee myös ottaa huomioon riskin kriittisyys hankkeen läpiviennissä. Usein voi olla hyötyä muiden vastaavien hankkeiden riskianalyysien tarkastelusta.

Arviointi voidaan tehdä taulukossa, josta on esimerkki alla.

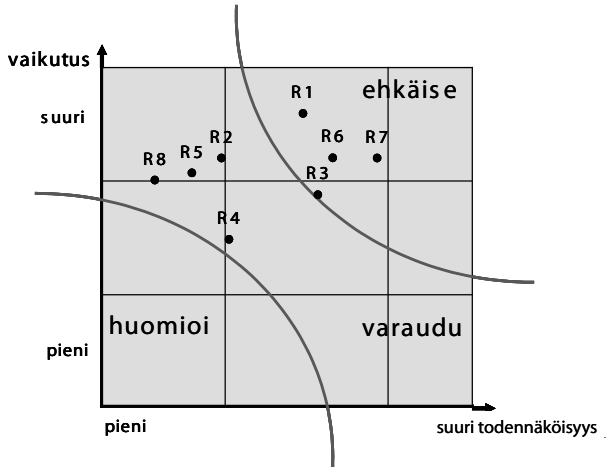
| | Rriskin nimi/ kuvaus | T 1) | V 1) | T x V 1) | keskeiset toimenpiteet riskin ehkäisemiseksi | Omistaja/ seuraaja | Kehitys suunta 2) |
|---|---|---|---|---|---|---|---|
| R1 | Tietoturvataso on määritetty liian tiukaksi ⟹ käsittelysääntöjä ei noudateta tai työ vaikeutuu | 1 | 3 | 3 | - Tarkastetaan ohjeisto<br>- Koulutetaan henkilöstöä<br>- Valvotaan tilannetta ja korjataan tarpeen mukaan | hankepäällikkö, konsultti valmistelee | |
| R2 | | | | | | | |
| R3 | | | | | | | |
| R4 | | | | | | | |

Riski = asia joks estää projektin tuotosten ja tulosten aikaansaamisen suunnitelman mukaan

1) Jos projektiryhmä katsoo tarpeelliseksi arvioida riskin todennäköisyyden T ja vaikutuksen V asteikolla 1-3

2) kasvaa, vähenee: voit esittää kehityssuunnan myös graafisesti seuraavalla sivulla

Arvioinnissa tulee käyttää myös desimaaleja erottelevuuden parantamiseksi. Riskit voidaan lajitella graafin avulla ja priorisoida riskienhallintaa vakavimpaan luokkaan. Seuraavassa kuvassa on esimerkki graafista ja riskien jakamisesta luokkiin.




Oleellista on kohdistaa ehkäiseviä toimenpiteitä ainakin vaikutuksiltaan vakavimpiin ja todennäköisimpiin riskeihin. Näistä ehkäisevistä toimenpiteistä voidaan tarvittaessa laatia esitettyä taulukkoa laajempi suunnitelma. Usein kuitenkin jo riskien tiedostaminen hankeorganisaatiossa johtaa siihen, että niitä vastaan suojaudutaan kaikilla tasoilla. Toimenpiteet on käynnistettävä välittömästi, niitä on toteutettava aktiivisesti ja niiden vaikutuksia on seurattava.

### 3.1.3 Tietoturvallisuuden organisointi

Tietoturvallisuus tulee vastuuttaa selkeästi eri osapuolille. Hankepäällikkö suunnittelee vastuiden jaon ja ohjausryhmä hyväksyy sen.

Lähtökohtaisesti tietoturvallisuuden kokonaisuudesta vastaa hankepäällikkö, joka voi jakaa tehtäviä hankehenkilöstölle. Hankepäällikkö vastaa siitä, että hankehenkilöstö on ohjeistettu, koulutettu ja valtuutettu hankkeessa käsiteltäviin tietoturvakäytäntöihin. Hankepäällikkö vastaa myös siitä, että henkilöstöllä on riittävät edellytykset toteuttaa tietoturvallisuutta muun muassa laitteiden ja tilojen osalta.

Tiedon turvaluokittelusta vastaa hankepäällikkö, joka on kaiken hankkeessa tuotetun tiedon omistaja. Työryhmissä tai osahankkeissa toimiva tiedon tuottaja luokittelee tiedon hankkeen ohjeiden mukaisesti. Työn tuotoksia hyväksyt-

täessä esimerkiksi ohjausryhmässä, vahvistetaan samalla turvallisuusluokitus. Hyväksytyn työn omistaa hyväksyjä.

JulkL:n tarkoittamia hankkeen asiakirjoja ovat ne, jotka hankepäällikkö toimittaa toimeksiantajalle hankkeen päätyttyä tai sen aikana.

Muut valmisteluryhmän omassa työssään käyttämät aineistot ovat JulkL 5.3§ 2 ja 3 kohdan tarkoittamia aineistoja. Nämä aineistot ovat 1) viranomaisen palveluksessa olevan tai viranomaisen toimeksiannosta toimivan laatimia muistiinpanoja taikka sellaisia luonnoksia, joita laatija ei ole vielä antanut esittelyä tai muuta asian käsittelyä varten, 2) viranomaisen sisäistä koulutusta, tiedonhakua tai muuta niihin verrattavaa sisäistä käyttöä varten hankittuja asiakirjoja;

Hankkeen sisäinen aineisto tulee merkitä niin, että sen luonne hankkeen sisäisenä valmisteluaineistona käy ilmi. Hankkeessa käytettävät viranomaisen asiakirjat täytyy merkitä siten, että niiden luonne erottuu hankkeen muusta (sisäisestä) materiaalista.

Hankehenkilöstö vastaa siitä, että ohjeet on omaksuttu ja niitä noudatetaan kaikissa työn vaiheissa. Henkilöstön tulee myös tuoda esille havaitsemansa epäkohdat ja kehittämiskohteet. Hankehenkilöstölle on suositeltavaa laatia tiivistetty toimintatapaohje yleisempiä tapauksia varten. Hankkeen hyvä ja tietoturvallinen toimintamalli on tärkeä elementti.

Hankepäällikkö valvoo tietoturvallisuuden toteutumista työhön osallistujien, tietoteknisten järjestelmien ja palvelujen, ulkopuolisten toimijoiden sekä hankkeen tuotosten osalta.

Tietoturvarikkeissä ja käsittelyvirheissä havaitsija estää tapahtuman ja sen leviämisen, ilmoittaa asiasta hankepäällikölle sekä dokumentoi tapahtuman tarkasti. Hankepäällikkö informoi näistä tilanteista niitä, joiden toimintaan rike tai tapahtuma vaikuttaa. Hankepäällikkö on vastuussa tietoturvajärjestelyjen kehittämisestä siten, että tapahtuma ei pääse toistumaan sekä käynnistämään mahdolliset tutkintatoimet ja vahingoista toipumisen. Tapahtumien dokumentointi on erityisen tärkeää niissä tapauksissa, joissa voidaan soveltaa palvelusopimukseen perustuvaa toimittajan sanktiota. Tapauksia saatetaan joutua käsittelemään myös oikeudessa.

Tietoturvarikkeitä valvovat käytettävien järjestelmien valvonnasta, työtiloista tai työprosesseista vastaavat henkilöt tai organisaatiot. Yleensä pyritään noudattamaan näiden tapahtumien hallinnan ja toipumisen menettelyjä. Rikkeistä ilmoitetaan hankepäällikölle. Asiasta on sovittava otettaessa järjestelmää tai palvelua käyttöön.

Tietoturvallisuuden vaatimustasoa, käsittelysääntöjä sekä tarkastamista ja auditointia määriteltäessä noudatetaan mahdollisimman pitkälle tietoturvastandardeja, ohjeita tai valtiohallinnossa vakiintuneita hyviä käytäntöjä.

Arvioitaessa organisaatioiden tietoturvallisuuden johtamisen kypsyyttä tai toteutuksen tasoa, voidaan se osin perustaa mahdolliseen saavutettuun ja auditoituun tietoturvasertifikaattiin. Tässä on kuitenkin huomioitava, että yhteisen rakenteen ja kriteeristön puuttuessa hankekohtaiset määrittelyt ovat määrääviä.

### 3.1.4 Toiminnalliset vaatimukset tietoturvallisuudelle

Hankkeelle tulee asettaa sen läpiviennin kannalta toiminnalliset vaatimukset, joihin tietoturvallisuuden toteuttaminen tähtää. Toiminnallisissa vaatimuksissa tarkastellaan lähinnä niitä hankkeen läpiviennin ja työprosessin kannalta oleellisia asioita, joihin tietoturvallisuudella voi olla edistäviä tai haittaavia vaikutuksia. Tietoturvallisuuden toteuttamisessa nämä pyritään ottamaan huomioon kuitenkaan tietoturvallisuutta vaarantamatta.

### 3.1.5 Hankkeen tietoaineiston varmistaminen

Jatkuvuuden varmistamiseksi on työssä tuotettujen tietojen varmistaminen sovittava ja ohjeistettava tarkoin. Hankkeen kannalta on tarkoituksenmukaista, jos hankkeen tiedot voidaan säilyttää sellaisissa ympäristöissä, joissa normaalissa toimintaprosessissa on järjestetty varmistaminen. Mikäli tämä ei tietoturvasyistä ole mahdollista, tulee varmistaminen järjestää hankkeen toimenpitein. Varmistamisessa tulee ottaa huomioon myös tiedon saatavuus esimerkiksi henkilökohtaisilta levyalueilta.

Hankkeessa tarvittavan osaamisen varmentamista voidaan edistää sopimusmenettelyllä. Yleensä laitteistoja ei ole tarpeen varmentaa.

Yhteinen sähköinen työtila (esimerkiksi organisaation käyttämä Sharepoint) on normaalisti palvelu. Tämän palvelun osana tulee olla tallennettavien tietojen varmentaminen.

## 3.2 Yritys- ja henkilöstöturvallisuus

Yrityksiltä edellytetään valtionhallinnon organisaatioiden ja henkilöiden kaltaista sitoutumista sekä auditointimahdollisuutta. Laajemmissa hankkeissa ja pidempiaikaisissa yhteistoimintasuhteissa tulee yritysten kanssa pyrkiä laatimaan erillinen yritysturvallisuussopimus. Mallina voidaan käyttää puolustusvoimien yritysturvallisuussopimusmenettelyä, jossa laaditaan yleinen yritysturvallisuussopimus velvoitteineen sekä sen täydennykseksi hankekohtainen liite.

Menettelyyn kuuluu myös yritysturvallisuuden auditointi. Sopimuksia laadittaessa suositellaan pysyttäväksi mahdollisimman pitkälle valtionhallinnon laatimassa mallisopimuspohjassa. Muussa tapauksessa voidaan joutua tilanteeseen jossa yrityksen samalla henkilöstöllä on pahimmillaan noudatettavana useampia toisistaan poikkeavia sopimuksia.

Turvallisuusluokiteltuun hankkeeseen osallistuvasta valtiohallinnon ulkopuolisesta henkilöstöstä tulee hankkeessa olla tehtynä joko suppea tai perusmuotoinen turvallisuusselvitys riippuen tiedon käsittelyn asettamista vaatimuksista.

Kaikilta henkilöiltä edellytetään myös hankekohtainen vaitiolositoumus (NDA), joka on liitteenä 3. Vaitiolositoumuksella vahvistetaan se, että henkilö tietää velvollisuutensa ja tuntee hankkeen tietoturvakäytännöt.

Hankkeen henkilövaihdot ovat mahdollisia ainoastaan hankepäällikön luvalla. Tällöin hankepäällikkö varmistaa turvaselvityksen ja teettää vaitiolositoumuksen.

Hankkeisiin kohdistuu eri syistä ulkopuolista mielenkiintoa. Näissä tapauksissa hankepäällikkö päättää kenelle hankkeen tietoja voi luovuttaa ja tarvittaessa suorittaa luovutukset itse. Kaikki hanketta koskeva tiedottaminen on hankepäällikön vastuulla, eikä hankkeessa kukaan tiedota asioita ilman hankepäällikön valtuutusta.

Matkustettaessa yleisissä kulkuneuvoissa tai oleiltaessa yleisissä tiloissa tulee hankkeen luottamuksellisia tietoja kuljettaa suojattuina sekä käsitellä siten, että ulkopuoliset eivät niitä saa tietoonsa.

## 3.3 Tietoaineistoturvallisuus

Hankkeessa tuotettava tai käsiteltävä tietoaineisto turvallisuusluokitellaan. Hankkeen käyttöön saadussa lähdeaineistossa noudatetaan tiedon omistajan luokittelua, merkintätapoja ja sitä vastaavia käsittelysääntöjä. Mikäli merkinnöissä on väärinkäsityksen mahdollisuus, lähdeaineisto tulee varustaa hankkeen turvallisuusluokitusmerkinnöillä.

Hankkeen tuottama aineiston luokittelee aineiston tuottaja ja sen vahvistaa hankepäällikkö. Hankkeessa tuotettu tietoaineisto luokitellaan ja merkitään valtionhallinnon voimassa olevan käytännön mukaisesti. Mikäli materiaalia ei ole merkitty turvallisuusluokitelluksi, sitä voidaan käsitellä julkisena. Tiedon hankkeen aikaisesta julkisuudesta tulee aina varmistua erikseen.

Merkintöjen tulee olla asetuksen mukaiset. Jos asiakirjat leimataan, on aina merkittävä julkisuuslain 24 §:n kohta, johon leimaaminen perustuu.

Hankepäällikkö määrittää sellaisten käsiteltävien tietojen korkeimman suojausluokan, jota voidaan hankekohtaisten ohjeiden ja menettelyjen perusteella käsitellä ilman erityistoimenpiteitä. Korkeamman suojausluokan materiaalin käsittelylle on määritettävä tapauskohtaiset erilliset menettelyt, joiksi voidaan osoittaa esimerkiksi jonkin hankkeeseen osallistuvan organisaation menettely ja ohjeistus.

Materiaaleja säilytetään suojausluokan vaatimissa tiloissa.

Dokumenttien kuljettamisessa on noudatettava asiaan kuuluvaa huolellisuutta. Tietovälineissä säilytettävä ja kuljetettava suojaluokiteltu tietoaineisto on suojattava valtiohallinnossa hyväksytyllä menettelyllä.

Hankkeessa käsiteltävän salaisen ja erittäin salaisen tiedon käsittely tulee ohjeistaa erikseen.

Dokumentit voidaan hävittää hankkeeseen osallistuvien organisaatioiden tietoturvamateriaalin hävittämismenettelyillä, yleensä silppuamalla vaatimukset täyttävällä silppurilla.

## 3.4 Fyysinen turvallisuus

Tilojen, joissa työtä tehdään, on oltava äänieristykseltään, näkösuojaltaan, kulunvalvonnaltaan ja murtosuojaukseltaan sellaiset, että niissä käsiteltävän tiedon joutuminen hankkeen kannalta ulkopuolisen haltuun ei ole mahdollista.

Tilojen valinnassa ja käytössä on huomioitava tietojen suojausluokan vaatimukset.

Työn tekemistä johtava henkilö vastaa siitä, että tilat täyttävät edellä kuvatut vaatimukset, ja ettei tilojen käytön loppuessa niihin jää mitään tietoturvallisuuden kannalta arkaa materiaalia. Työtä voidaan tehdä virastoissa tai ulkopuolisissa tiloissa, jotka täyttävät edellä kuvatut vaatimukset.

## 3.5 Ohjelmistoturvallisuus

Työssä käytetään organisaatioiden sopimia lisensioituja ohjelmistoja. Ohjelmistojen pitää olla turvapäivitettyjä ja ylläpidettyjä kunkin organisaation käytäntöjen mukaisesti. Mikäli työn tekemisen kannalta on välttämätöntä käyttää avoimen lähdekoodin ohjelmistoja, se sovitaan erikseen..

Sähköisissä dokumenteissa ei käytetä sellaisia ohjelmistojen omia suojausmenettelyjä, joiden muokkaus- tai käsittelysalasana on ainoastaan laatijan hallussa.

## 3.6 Tietoliikenneturvallisuus

Sähköpostilla välitettävä turvaluokiteltu tieto on suojattava salaamalla liitetiedostot itsepurkautuviksi paketeiksi, salaamisohjelmistojen omiksi tiedostomuodoiksi tai salaamalla koko sähköposti valtionhallinnossa käyttöön hyväksytyillä sovelluksilla tai menetelmillä, mm. sähköisen varmenteen sisältävällä virkakortilla.

Ennen menetelmän käyttöönottoa tulee selvittää sen soveltuvuus tietoliikennettä suodattaviin palomuureihin sekä käyttöliittymiin. Salaamiseen tarvittavin laitteiden ja ohjelmistojen hankinnoista tulee sopia hankekohtaisesti.

Hankkeen käyttöön voidaan avata sähköinen ryhmätyötila, jonka käyttö tulee ohjeistaa erikseen turvaluokitellun materiaalin osalta. Ryhmätyötilan käytöstä päättävät osallistuvat organisaatiot keskenään silloin kun se käyttö

on mahdollista. Tällöin vaihtoehtoina ovat käyttöoikeuksiin perustuva tietoturvallisuus tai liitetiedostojen tallentaminen salattuina.

## 3.7 Laitteistoturvallisuus

Laitteistoturvallisuudessa noudatetaan kunkin organisaation omaa tietoturvaohjeistusta ja menettelyjä.

## 3.8 Käyttöturvallisuus

Etätyössä noudatetaan kunkin organisaation omaa tietoturvaohjeistusta ja menettelyjä. Työryhmäympäristön käytössä on ohjeistettava niihin pääsy yleisistä verkkoympäristöistä.

# 4 Tiivistetyt tietoturvaohjeet hankkeeseen osallistujille

Hankkeeseen osallistuja perehdytetään hankkeen tietoturvaohjeeseen kokonaisuudessaan siten, että hän kykenee noudattamaan tietoturvaperiaatteita.

Ohjeistukseen ja perehdytykseen sisällytetään keskeisimmät tiivistetyt osallistujan ohjeet hankkeeseen liittymisestä, siinä työskentelystä sekä työskentelyn päättämisestä.

LIITE 1

# Esimerkki hankkeen tietoturvaohjeen sisällöstä

## SISÄLLYS

# 1 Johdanto

- Tietoturvaohjeen tarkoitus ja velvoittavuus (alkaa, päättyy, miltä osin jatkuu)
- Ohjeen perustedokumentit
- Ohjeen laatimisprosessi ja hyväksyntä
- Keskeiset luottamussuhteisiin vaikuttavat tekijät ja rajaukset
- Luettelo hankkeen kannalta oleellisista säädöksistä ja ohjeista (mm. VAHTI-ohjeet)
- Käytettävä keskeinen termistö
- Tietoturvaohjeen lukuopastus

# 2 Hankkeen kuvaus

- Hankkeen yleiskuvaus
- Hankkeen turvallisuusluokka
- Hankkeen johtamisen järjestelyt
- Vaiheistus tietoturvallisuuden kannalta
- Liittyminen muihin hankkeisiin, eri organisaatioiden tehtäviin, vaikutus tietoturvallisuuteen
- Hanketta edeltävät ja seuraavat vaiheet
- Tietoturvallisuuteen vaikuttavat tekijät (henkilöstö, organisaatiot, toimitilat, ulkopuoliset toimijat)

# 3 Tietoturvallisuus hankkeen eri vaiheissa

## 3.1 Tietoturvallisuuden johtaminen

- tavoiteltava tietoturvallisuuden taso ja sen rajaaminen
- tietoturvallisuuden johtamisen vastuut, päätöksenteko ja organisointi (ohjausryhmä, hankepäällikkö, osaprojektien vastaavat, asiantuntijat)
- turvallisuusluokittelun päätöksentekomenettely (työ-, väli- ja tulosdokumentit), vastuut ja oikeudet
- tietoturvallisuuden valvonta ja auditointi
- tietoturvallisuuden raportointi ja kehittäminen
- tietoturvaohjeen ylläpitäminen
- tietoturvaohjeen mukaisten toimenpiteiden toteuttaminen ja määriteltyjen edellytysten varmistaminen (operatiivinen toiminta)

## 3.2 Hankkeen perustaminen

- hankkeen uhka- ja tietoturvariskiarvio sekä riskien hallinta, arvion päivitysprosessi
    - hankkeessa käsiteltävät eri turvallisuusluokkien dokumentit sekä tietotekniset ympäristöt, mahdollisuus parantaa rakenteiden tietoturvallisuutta, keskeiset valinnat
    - toimitila- ja henkilöstöturvallisuuden taso ja sen parantaminen
    - tietoturvakulttuuri ja sen parantaminen
- tietoturvallisuutta koskevien toiminnallisten vaatimusten asettaminen
    - johtaminen

    - organisaatioiden osallistuminen
    - ulkopuolisten toimijoiden käyttö
    - toimitilat ja matkustaminen
    - turvallisuusluokiteltujen sähköisten ja paperidokumenttien käsittely ja säilytys
    - palvelujen käyttö (mm. työryhmätila, kyselyt, verkkoviestintä)
    - työprosessi (mm. etätyö, työskentely tietyssä tilassa)
    - viestintä
    - jatkuvuus ja toipuminen

- tietoturvakäytäntöjen määrittäminen siten, että jokainen hankkeeseen osallistuva organisaatio hyväksyy ne ja kykenee suhteuttamaan omat tietoturvaperiaatteensa niihin
    - henkilöstöturvallisuus, mm.:
        - taustaselvitykset
        - henkilövaihdot
        - sosiaalinen hakkerointi
        - tiedottaminen
        - matkustaminen
        - ulkopuolisen ja virkamiehen ero
    - tietoaineistoturvallisuus
        - turvaluokat - tietoaineisto
        - turvaluokat – tuotettavat dokumentit
        - dokumenttien säilyttäminen
        - dokumenttien kuljettaminen
        - dokumenttien hävittäminen
        - sähköiset aineistot
        - varmuuskopiointi
        - versiohallinta
    - fyysinen turvallisuus
        - lukitukset
        - kassakaapit

    - paloturvallisuus
    - kenen tiloissa toimitaan?
- ohjelmistoturvallisuus
    - sallitut ohjelmistot
    - kielletyt ohjelmistot
    - pakolliset ohjelmistot
    - harkinnanvaraisuus
- tietoliikenneturvallisuus
    - sähköposti
    - lähiverkot ja erillisverkot
    - ryhmätyötilat
- laitteistoturvallisuus
    - laitteiden (pc, muistitikku, irrotettava kovalevy, tulostin) käyttäminen muuhun työskentelyyn
    - verkkokäytön salliminen
    - laitteistoille ja varusohjelmille asetettavat vaatimukset (virustorjunnan päivitys, etähallinta)
    - laitteiden merkitseminen
    - laitteiden säilyttäminen
    - dedikoidut laitteet
    - laitteiden varmentaminen
- käyttöturvallisuus
    - etätyö
- tietoturvapoikkeaman käsittely ja toipuminen
    - tietoturvapoikkeaman käsittelyprosessi ja päätösmenettelyt
    - vahinkojen rajoittaminen, käyttöoikeuksien sulkeminen ja avaaminen
    - tietojen ja palveluiden palauttaminen
    - vahinkojen arviointi, tutkinta ja vaikutusten minimointi
    - tiedottaminen

- tietoturvaperiaatteiden ja -käytäntöjen hyväksyminen ja toimeenpano
- ennakkotoimenpiteiden toteuttaminen
    - henkilöstön turvallisuusselvitykset, NDA:t
    - yritysturvallisuusjärjestelyt
    - tietoturvaohjelmistojen, -laitteiden ja –palvelujen hankinnat
    - ohjeiden ja koulutusmateriaalien valmistelu
    - selvitykset ja testaukset
- jatkuvan ylläpidon ja valvonnan mekanismin luominen (muutoshallinta)

## 3.3 Ulkopuolisen asiantuntija valinta

- Mitä asioita otetaan erityisesti huomioon
    - kilpailuttamisvaiheessa
    - sopimusvaiheessa (velvoitteet, koulutus, valvonta, sanktiot)
    - alihankintaketjuissa (myös alihankintoina tehdyt ja alihankkijoiden hankkimat tukipalvelut, mm. siivous)
- yritysturvallisuussopimus
- turvallisuusselvitykset
- jatkuva valvonta
- vastuuhenkilöt ja -suhteet

## 3.4 Hankkeen käynnistäminen

- tietoturvaohjeistus tehty ja otettu käyttöön
- henkilöstön tarkastus
- koulutus ja perehdyttäminen (audit trail)
- tietoturvavastuiden vastaanotto aiemmalta vaiheelta
- materiaalien vastaanotto, tarkastaminen ja sovittaminen hankkeen tietoturvaperiaatteisiin
- mahdolliset muutokset aiempiin toimintatapoihin
- tulosten raportointi ja vahvistaminen

## 3.5 Hankkeen työskentely

- riskienhallinta
- valvonta
- raportointi
- ad hoc –tarkastukset
- virheisiin puuttuminen
- tietoturvaloukkaukset
- muutoshallinta (mm. henkilövaihdokset, käyttöoikeuksien hallinta, salasanojen vaihtaminen)
- yhteydenpito projektihenkilöstöön
- raportointi

## 3.6 Hankkeen valmistuminen

- hankejohdon vahvistus merkintöihin
- tulosten ja materiaalin luovuttamiseen liittyvät asiat
- dokumenttien hallinta tunnetaan

## 3.7 Hankkeen lopettaminen

- materiaalien luovuttaminen ja hävittäminen, raportointi
- materiaali siirretty organisaatio(ide)n vastuille
- tietoturvavastuiden jatkuminen
- hankkeen aikaisen tietoturvallisuuden raportointi
- kehittämisehdotusten laatiminen
- tietoturvavastuiden luovuttaminen

# 4 Tiivistetyt tietoturvaohjeet hankkeeseen osallistujille

- hanketyöskentelyn aloittaminen
    - vastuut
    - ohjeet
    - käytännön järjestelyt
- hanketyöskentely
    - keskeiset ohjeet
- hanketyöskentelyn päättäminen
    - toimenpiteet
    - vastuut

LIITE 2

# Hankkeen tietoturvaohje

## Esimerkki

## SISÄLLYS

# 1 Johdanto

Tämä tietoturvaohje on tarkoitettu noudatettavaksi hankkeessa aikavälillä (pvm. 1 – pvm. 2). Hankkeen tietoturvaohjetta noudatetaan soveltuvilta osin hankkeen tuottamiin materiaaleihin kunnes ne luovutetaan valiovarainministeriölle tai hankkeen seuraavalle vaiheelle.

Ohje perustuu laatimishetkellä voimassa olevaan säädäntöön ja VAHTI-ohjeistoon. Niiltä osin kuin edellä mainituissa dokumenteissa ei ole asioita käsitelty, on pyritty noudattamaan hyviä tunnettuja käytäntöjä.

Ohje on laadittu toimittajan tuella ja sitä on käsitelty keskeiset hankkeeseen osallistuvat osapuolet kattavassa valmisteluryhmässä. Ohjeen on hyväksynyt käyttöön otettavaksi hankkeen ohjausryhmä kokouksessaan (pvm.).

Tietoturvaohjeen hyväksyminen, noudattaminen ja tämän valvonta muodostavat perustan sille, että organisaatiot voivat luovuttaa hankkeen käyttöön sen tarvitseman materiaalin. Näin voidaan myös turvata hankkeen tuottaman materiaalin luottamuksellisuus materiaalin koko elinkaaren ajan.

Ohjeessa käytetään VAHTI-ohjeiston mukaista termistöä.

Tietoturvaohje on tarkoitettu jokaisen hankkeeseen osallistuvan luettavaksi kokonaisuudessaan. Luvussa 4 korostetaan vielä tärkeimpiä hankkeeseen osallistujan huomioon otettavia asioita.

# 2 Hankkeen kuvaus

Hanke alkaa (pvm.) ja päättyy (pvm.). Hanketta on edeltänyt erilaisia esitutkimuksia ja se tulee jatkumaan määrittely- ja toteutusvaiheeseen useissa valtionhallinnon erillisissä hankkeissa sekä mahdollisissa omissa jatkohankkeissa.

Hanke liittyy valtionhallinnon yhteisiin ja hallinnonalakohtaisiin vastaaviin hankkeisiin ja pyrkii hyödyntämään näissä sekä aiemmin hallinnossa tuotettuja tietoja ja rakenteita mahdollisimman paljon.

Hanke on tilaajan johtama poikkihallinnollinen hanke, jossa osallistujia on useilta eri hallinnonaloilta ja –tasoilta. Hanketta tuetaan ulkopuolisen konsultin työllä.

Hanketta ohjaa tilaajan johtama ohjausryhmä. Päävastuussa toteutuksesta on päätoiminen hankepäällikkö, jolla on apunaan valmisteluryhmä. Laaja-alaista näkemystä ja informaatiota välitetään suurehkon seurantaryhmä avulla. Näiden lisäksi hanke voi käyttää hallinnonaloilta erikseen nimettyjä asiantuntijoita.

Työhön osallistuvat ryhmät ja henkilöt vaihtavat informaatiota sähköpostitse, kokouksissa, wiki-palvelussa sekä käyttöön otettavassa tilaajan työryhmäohjelmistossa, johon on pääsy kaikilla henkilökohtaisen käyttäjätunnuksen ja salasanan avulla. Hankkeen käyttöön kerättävä materiaali, työmateriaali ja tuotokset pyritään myös kokoamaan työryhmäohjelmistoon kaikkien käytettäväksi. Osin materiaali kerätään tietoturvasyistä hankepäällikön haltuun.

Työskentely tapahtuu sekä valtionhallinnon että ulkopuolisissa tiloissa. Työskentelystä merkittävä osa on siis erilaista etätyötä, jossa pyritään käyttämään mahdollisimman paljon yhteisiä tietovarantoja. Hankkeella ei ole erityisiä ohjelmistoja, laiteympäristöjä tai konfiguraatioita. Hankkeessa käytetään normaaleja työskentelyresursseja ja yleisesti käytettyjä työkaluja.

# 3 Tietoturvallisuus hankkeen eri vaiheissa

## 3.1 Tietoturvallisuuden johtaminen

Hanke luokitellaan luottamuksellisuudeltaan luokkaan ”Käyttörajoitettu”. Hankeen turvallisuusjärjestelyt on näin ollen suunniteltu luottamuksellisuuden osalta täyttämään tämä luokan vaatimukset ja hanke tähtää lopputulokseen, jonka tiedon taso on ”Käyttörajoitettu”. Tämä tarkoittaa sitä, että muun muassa tietotekniikka, lähdemateriaali, tuotosten tietosisällöt, henkilöstö ja jakelut mitoitetaan tämän mukaisesti.

Erityisissä tapauksissa jouduttaneen käsittelemään ja tuottamaan materiaalia, joka on korkeampaa tietoturvaluokkaa. Näistä tapauksista päättää hankepäällikkö ja näihin sovelletaan VM:ssä käytössä olevaa tietoturvaohjeistusta.

Ohjausryhmä on hyväksynyt tässä ohjeessa esitetyt tietoturvallisuuden periaatteet. Hankepäällikkö vastaa kokonaisuudessaan periaatteiden toteuttamisesta hankkeessa, valvoo sitä sekä raportoi tietoturvallisuudesta säännöllisesti ohjausryhmälle. Hankepäällikkö voi jakaa tietoturvallisuustehtäviä osaprojektien johtajille tai muulle asiantuntijahenkilöstölle. Hankkeeseen osallistujat vastaavat ohjeiden noudattamisesta sekä normaalista virheiden havainnoinnista.

Hankepäällikkö vastaa hankkeen käyttöön saadun materiaalin sovittamisesta hankkeen tietoturvaluokitteluun. Pyrkimyksenä on, että hankkeen tietoturvaperiaatteet yhdentyvät niin paljon muiden valtionhallinnon organisaatioiden tietoturvaluokitteluun, että sovittaminen on selkeää.

Hankkeessa tuotettavan materiaalin luokittelee työvaiheessa materiaalin tuottaja. Kirjattavien väli- ja lopputuotosten luokittelun vahvistaa hankepäällikkö.

Hankepäällikkö vastaa tietoturvallisuuden valvonnasta sekä hallinnonaloille ja ulkopuolisille toimijoille tehtävistä auditoinneista ja tarkastuksista ennen hankkeen työn aloittamista ja sen aikana. Hankepäällikkö vastaa myös havaittujen virheiden korjauttamisesta, riskien poistamisesta sekä mahdollisten muiden jälkitoimenpiteiden käynnistämisestä.

Hankepäällikkö kerää hankkeen aikana erilaisia yleisesti hankkeen tietoturvallisuuden kehittämiseen liittyviä käytäntöjä ja sisällyttää ne hankkeen päättyessä hankkeiden tietoturvallisuuden käsikirjaan. Hankkeen päättyessä hankepäällikkö laatii loppuraportin osaksi myös tietoturvallisuutta käsittelevän kohdan.

Hankepäällikkö varmistaa ennen hankkeen alkamista, että hankkeella on kaikki edellytykset, jotka vaaditaan tämän tietoturvaohjeen noudattamiseen. Näitä ovat erityisesti hankesuunnitelma, henkilöstö sekä tietotekniset resurssit. Hankeen aikana hankepäällikkö vastaa reagoimisesta havaittuihin tietoturvatapahtumiin, niiden vaikutusten minimoimisesta, toipumisesta sekä tiedottamisesta.

## 3.2 Hankkeen perustaminen

Hankkeen keskeisimmät riskit arvioidaan hankkeen alussa, tietoturvariskit mukaan luettuina. Riskit kirjataan erilliselle riskienhallintalomakkeelle, jossa myös niiden suuruus ja kriittisyys arvioidaan. Merkittävien riskien poistamiseksi tehdään suunnitelma toimenpiteistä.

Hankkeessa käsitellään julkisen lisäksi tietoaineistoja, joka on merkitty eri hallinnonaloilla pääasiassa luokkiin ”TTL III luottamuksellinen” ja TTL IV ”käyttörajoitettu”, ”viranomaiskäyttö” tai ”ei tietoa sivullisille”.

TTL II luokkaan ”salainen” tai TTL I luokkaan ”erittäin salainen” tai ”vain nimettyjen henkilöiden tietoon” merkittyä materiaalia käsitellään vain erityistapauksissa ja tapauskohtaisesti.

Hankkeen merkittävimmät tietoturvariskit ovat:

- Hankkeessa käsiteltävää tai luotua luottamuksellista tietoa joutuu hallitsemattomasti ulkopuolisten tahojen haltuun.
  Tämä voi estää materiaalin käyttöön saamista tai vaarantaa hankkeen piirissä olevia toimintoja.
- Valtuuttamattomat henkilöt pääsevät hankkeen työryhmäohjelmistoon ja sitä kautta systemaattisesti hankkeen tietoihin.
  Vaikutus on kuten edellä, mutta pitkäaikaisesti.
- Hankkeen käyttöön saadut tiedot eivät ole kaikkien käytettävissä.
  Vaikutus kohdistuu hankkeen tuloksiin.
- Hankkeen tuotoksia menetetään rajatuksi ajaksi tai kokonaan.
  Hankkeen työprosessi viivästyy ja vaikeutuu tai työvaiheita joudutaan uusimaan kokonaan. Hankkeen aikataulu on hyvin kriittinen eikä kestä viiveitä ilman lopputulosten laadun merkittävää putoamista.

- Hankkeessa työskentelevien henkilöiden turvallisuutta ei ole tarkastettu tai tarkastuksissa on ilmennyt ongelmia.
  Hanke saattaa viivästyä tai menettää merkittävää asiantuntemusta.
  Voi aiheuttaa tietovuotoriskin.
- Hankkeen työmateriaalien tai tuotosten tietoturvamerkinnät ovat puutteellisia. Materiaaleja ei käsitellä oikein ja niitä voi joutua asiankuulumattomiin käsiin.
- Materiaalien säilytys ja versiohallinta eivät toimi.
  Työprosessissa menetetään tehokkuutta, koska muun muassa kommentointi perustuu eri versioihin. Pahimmillaan kehittäminen tapahtuu rinnakkain kahden version kanssa.

Kiinnittämällä erityistä huomiota yksilötasolla hankkeen tietoturvallisuusohjeistukseen ja -riskeihin voidaan kehittää hyvää tietoturvakulttuuria ja pienentää riskien toteutumisen todennäköisyyttä. Hyvään tietoturvakulttuuriin kuuluu myös havaittujen omien ja muiden virheiden esille tuominen ja siten niiden toistumisen estäminen.

### 3.2.1 Toiminnalliset vaatimukset

Hankkeen tietoturvallisuudelle voidaan asettaa seuraavat toiminnalliset vaatimukset:

1. Tietoturvallisuutta tulee johtaa selkeästi ja määrätietoisesti sovittujen periaatteiden mukaisesti. Tietoturvallisuuden johtamisen, toteuttamisen ja valvonnan on oltava hankkeeseen osallistuvien tahojen kannalta luotettavaa ja rinnastettavissa näiden omaan tietoturvallisuuden johtamiseen.
2. Tietoturvallisuuden on mahdollistettava hankkeeseen osallistuvien organisaatioiden luottamus hankkeen toimintaan sekä myös muista organisaatioista hankkeeseen osallistuvien toimintaan.
3. Hallinnon ulkopuoliset toimijat on sitoutettava vaitiolomenettelyin ja sanktioin sekä yksilö- että yritystasalla hankkeen tietoturvallisuuteen.
4. Hankkeen on voitava käyttää työtiloinaan hallinnon tiloja. Työn on oltava mahdollista myös etätyönä ja ulkopuolisissa tiloissa.
5. Tietoteknisten alustojen ja palvelujen on täytettävä ”Käyttörajoitettu”-luokkaan turvaluokiteltujen sähköisten ja paperimateriaalien luomisen, viestittämisen, käsittelyn, säilyttämisen ja hävittämisen osalta sellaiset tietotuvallisuuden ominaisuudet, että työprosesseja voidaan toteuttaa turvallisesti ja joustavasti.

6. Tietoturvallisuusloukkaukset, -virheet sekä kehittämisen kohteet on voitava tunnistaa ja poistaa hankkeen kuluessa.
7. Työprosessin on voitava jatkua kitkatta ongelmatilanteiden ilmentyessä lyhyen toipumisajan jälkeen. Työprosessin vaiheen uusimista vaativia tilanteita ei saa syntyä.
8. Tietoturvallisuustilanteesta on raportoitava säännöllisesti työn ohjausryhmälle ja erityistilanteista on viestitettävä työhön osallistujille.

### 3.2.2 Tietoturvakäytännöt

Tietoturvakäytännöissä noudatetaan yleisesti käytettyjä periaatteita siten, että säädännön, valtionhallinnon normien ja suositusten (erityisesti VAHTI-ohjeet) vaatimukset täyttyvät. Seuraavassa korostetaan ja tarkennetaan eräitä käytännön seikkoja tässä hankkeessa.

Tämä ohje koskee tietojen käsittelyä, jotka ovat luokkaa ”käyttörajoitettu”. Luokka ”salainen” ja ”erittäin salainen” käsitellään erikoistapauksina valtiovarainministeriön ohjeiden mukaan.

**Henkilöstöturvallisuus:**

1. Hallinnon ulkopuolisesta henkilöstöstä tehdään perusmuotoinen turvallisuusselvitys viranomaisten ohjeistamalla menettelyllä. Hallinnon henkilöstöstä selvitetään, onko perusmuotoinen turvallisuusselvitys tehty ja se tehdään hankepäällikön harkinnan mukaan.
2. Kaikki hankkeeseen osallistuvat tekevät vaitiolovakuutuksen ennen luottamuksellisen materiaalin käsittelyä. Lomake on liitteenä.
3. Jokaiselle hankkeeseen osallistuvalle perehdytetään velvollisuudet tietoturvallisuuden osalta ja perehdyttämisestä pidetään kirjaa.
4. Hankepäällikkö vastaa edellä mainittujen toimenpiteiden toteuttamisesta mahdollisten uusien henkilöiden liittyessä työskentelyyn.
5. Hankkeen tietoja saa käsitellä ainoastaan turvaluokitellun virastotyön vaatimukset täyttävissä tiloissa ja hankkeeseen kuuluvien henkilöiden kanssa. Erityisesti julkisia tiloja ja sosiaalista hakkerointia tulee varoa.

**Tietoaineistoturvallisuus:**

1. Tietoaineisto luokitellaan ja merkitään hankkeessa seuraaviin luokkiin (saatavissa piirrosobjekteina työryhmäympäristöstä):




2. Luokittelusta vastaa materiaalin tuottaja. Tuloksia vahvistettaessa luokituksen vahvistaa hankepäällikkö.
3. Hankkeen vastaanottaman materiaalin osalta luovuttajan ja hankkeen luokituksen keskinäisestä rinnastamisesta vastaa hankepäällikkö. Tarvittaessa materiaali merkitään selkeästi hankkeen tietoturvamerkinnöin.
4. Merkintävelvoite koskee paperidokumentteja, sähköisiä dokumentteja, tiedostoja sekä irrotettavia muistivälineitä. Sähköisiin dokumentteihin (mm. Word ja PowerPoint) merkitään yllä kuvattu leima, tiedostonimeen liitetään lyhenne (KÄYRAJ, LUOTT, SAL, ERITTSAL). Julkisia materiaaleja ei merkitä. **Merkitsemättömiä materiaaleja käsiteltäessä ja jaettaessa tulee aina varmistua sisällön julkisuudesta.**
5. Turvaluokiteltua (TTL IV) materiaalia tulee säilyttää suojausluokan IV mukaisesti suojatuissa tiloissa. Sähköisten dokumenttien säilyttämiseen ja siirtämiseen käytetään organisaatioiden käyttämiä massamuistien salaamisohjelmistoja tai salaavia muistivälineitä. Yhtei-

sillä levyalueilla materiaalin säilyttäminen on kiellettyä. Paperidokumentteja säilytetään valvotuissa tiloissa lukituissa kaapeissa. Erityistä huomiota tulee kiinnittää tietoverkon yli automaattisesti suoritettavaan kannettavien tietokoneiden tiedostovarmentamiseen yhteisille varmennusalueille.

6. Matkustettaessa tulee tietojen olla suojattuina; paperidokumenttien valvottuina ja sähköisten muistivälineiden suojattuina salaamisohjelmistoin. Luokkaa ”salainen” ja ”erittäin salainen” olevia materiaaleja ei saa säilyttää salaamattomana.
7. Sähköisten työympäristöjen käyttäjätunnusten ja salasanojen säilyttämiseen on kiinnitettävä erityistä huomiota, niiden luovuttaminen muille on kiellettyä.
8. Materiaalit hävitetään turvallisesti noudattaen kunkin osallistuvan organisaation turvamateriaalin hävittämisestä annettuja menettelytapaohjeita. Materiaalin hävittäminen raportoidaan hankepäällikölle hankeen lopussa. Hävittäminen koskee myös sähköisiä materiaaleja, tarvittaessa irrotettavia muistivälineitä sekä varmuuskopioita.
9. Kaikkien materiaalien saatavuus on turvattava. Hankkeeseen saadun materiaalin osalta riittää lähdetietojen varmuuskopiointi. Itse tuotetttu materiaali varmuuskopioidaan vähintään yhteen fyysisesti erillään olevaan paikkaan.

**Fyysinen turvallisuus:**

1. Materiaalit säilytetään joko paloturvallisissa kassakaapeissa tai jatkuvasti valvotuissa tiloissa lukitussa kaapissa.
2. Työskentely on mahdollista hankkeeseen osallistuvien normaaleissa työskentelytiloissa. Käyttörajoitettu-luokitusta korkeampien materiaalien käsittely on madollista ainoastaan hankepäällikön erikseen ohjeistamalla tavalla.
3. Toimittaessa normaalien työtilojen ulkopuolella, järjestetään normaaleja työskentelytiloja vastaavat tietoturvallisuusolosuhteet, muun muassa lukitukset, salakatselun ja –kuuntelun estäminen, tilojen valvonta, etukäteis- ja jälkitarkastus, roskien hävittäminen sekä kulun valvonta.

**Ohjelmistoturvallisuus:**

1. Hankkeessa käytetään ainoastaan organisaatioissa käytettäviä, valvottuja, vakioituja ja ylläpidettyjä käyttöympäristöjä.
2. Käyttöympäristöihin ei saa olla asennettuina ohjeiden vastaisia, tietoturvallisuutta heikentäviä ohjelmistoja ja perusalustojen tulee olla tietoturvan osalta päivitettyjä.

3. Käytettävien ohjelmistojen pitää olla lisensioituja ja virallisia versioita.
4. Käytettävät ohjelmistot ovat MS-Office, Adobe Acrobat ja Sharepoint. Harkinnanvaraisesti yksittäisissä työvaiheissa voidaan käyttää muita ohjelmistoja (muun muassa MindManager), mutta tällöin tuotokset on muunnettava käytettävien ohjelmistojen hyväksymään muotoon.
5. Vaihdettavien tiedostojen tallennusmuoto on .rtf tai .pdf. Makrojen ja muiden suoritettavien koodien käyttö tiedostoissa ei ole sallittua.

**Tietoliikenneturvallisuus:**

1. Tiedon välittämiseen käytetään pääasiassa sähköpostia ja yhteistä työryhmäohjelmistoa.
2. Käyttörajoitettu tieto tulee salata liitetiedostona itsepurkautuvaksi paketiksi ja nimetä uudelleen muotoon .ex_. Myös toimikorttipohjaista tiedostosalausta on mahdollista käyttää, mikäli osapuolilla on tähän tarvittavat kortit ja laitteet. Hankkeeseen osallistuvat hankkivat itse tarvittavat sovellukset ja sopivat palomuurisäännöstöjen sovittamisesta siten, että tiedonvaihto on mahdollista.
3. Kaikissa tapauksissa salattu tiedosto ja salasana on välitettävä eri mediaa käyttäen. kahdessa erillisessä sähköpostissa tiedon ja salasanan lähettäminen ei ole sallittua. Työvaiheissa voidaan sopia vakiosalasanat, jota kuitenkin tulee vaihtaa kuukausittain.
4. Työryhmäohjelmistoon voidaan taltioida ja sieltä noutaa korkeintaan ”käyttörajoitettu”-luokan materiaalia ilman erillistä salaamista.

**Laitteistoturvallisuus:**

1. ”Käyttörajoitettu”-luokan materiaalia saa käsitellä normaalissa työympäristössä.
2. Irrotettavien muistivälineiden käyttäminen muuhun työskentelyyn on kiellettyä. Hankkeessa luovutetaan käyttäjille tarpeen mukaan salaava muistitikku.
3. Yhteisten levyalueiden käyttö hankkeen materiaalien varastoimiseen edes varmennustarkoituksissa on kielletty. Poikkeuksena on työryhmäohjelmisto.
4. Käytettävien laitteistojen on oltava vakioituja sekä jatkuvan ylläpidon ja tietoturvapäivitysten piirissä. Käyttäjän valvomatonta etähallintamahdollisuutta niissä ei saa olla.

**Käyttöturvallisuus:**

1. Etätyö on tyypillinen hankkeen työmuoto ja siis sallittu. Etätyö ei edellytä yhteyttä muihin yhteisiin verkko- tai tietoresursseihin kuin työryhmäohjelmistoon, joka vaatii sen kaikissa tapauksissa.
2. Työryhmäohjelmiston käyttötoiminnoista vastaa sitä ylläpitävä organisaatio asetettamiensa tietoturvaperiaatteiden mukaisesti.
3. Työryhmäohjelmisto on suojattu käyttäjätunnuksella ja salasanalla, joka toimitetaan käyttäjille.

**Tietoturvapoikkeamien käsittely ja toipuminen:**

1. Yhteistä käyttöympäristöä (työryhmäohjelmisto) valvovan organisaation todetessa tietoturvaloukkauksen tämän tulee ilmoittaa siitä hankepäällikölle. Tiedottamisvelvoitteesta on sovittava erikseen. Valvonnasta vastaava organisaatio käynnistää suojautumismenettelyt ja toipumisen ohjeistuksensa mukaan. Hankepäällikkö arvioi hankkeen kannalta tilannetta ja käynnistää tarpeelliset toimenpiteet vahinkojen rajaamiseksi ja vahingoista toipumiseksi.
2. Hankkeeseen osallistujan kohdatessa tietoturvaloukkauksen, hän ryhtyy itse toimenpiteisiin oman organisaationsa ohjeistuksen mukaan ja informoi tästä hankepäällikköä.
3. Hankepäällikkö vastaa tiedottamisesta tarpeellisessa laajuudessa hankkeen johtoryhmälle ja hankehenkilöstölle.

**Tietoturvaperiaatteiden ja -käytäntöjen hyväksyminen ja toimeenpano:**

1. Hankepäällikkö esittelee tietoturvaperiaatteet hankkeen johtoryhmälle, joka hyväksyy ne käytettäväksi. Sellaisten hankkeeseen osallistuvien organisaatioiden, jotka eivät ole edustettuina ohjausryhmässä, tulee hyväksyä periaatteet erikseen.
2. Hankepäällikkö vastaa ohjeiden mukaisten toimenpiteiden valmistelusta, edellytysten luomisesta, suorittamisesta, johtamisesta ja valvonnasta.

**Ennen hankkeen aloittamista tehdään seuraavat toimenpiteet:**

- hankkeen tietoturvaohjeen laatiminen ja kommentointi osallistuvilla hallinnonaloilla ja muilla toimijoilla
- henkilöstön turvallisuusselvitykset, NDA:t
- yritysturvallisuusjärjestelyt
- tietoturvaohjelmistojen, -laitteiden ja –palvelujen hankinnat
- ohjeiden ja koulutusmateriaalien valmistelu
- selvitykset ja testaukset

**Jatkuvan ylläpidon ja valvonnan mekanismin luominen (muutoshallinta)**

1. Jokainen hankkeeseen osallistuja on velvollinen esittämään hankepäällikölle epäkohdat ja kehitysehdotukset.
2. Hankepäällikkö muuttaa välttämättömiltä osiltaan ohjetta ja menettelytapoja hankkeen aikana; muutokset dokumentoidaan.

## 3.3. Ulkopuolisen asiantuntija valinta

Hankkeeseen on kilpailutettu ulkopuolinen asiantuntija (Digia Oyj). Kilpailutuksessa ja toimitussopimuksessa on huomioitu:

- turvallisuuteen liittyviin vaatimuksiin sitoutuminen
- henkilöiden vaitiolositoumukset ja turvallisuusselvitykset
- säädännön asettamat velvoitteet
- salassapitovelvollisuus
- sanktiot sopimusrikkomuksista.

## 3.4 Hankkeen käynnistäminen

Ennen hankkeen käynnistämistä hankepäällikkö varmistaa suunniteltujen toimenpiteiden ja tietoturvaedellytysten toteutumisen. Keskeisiä näistä ovat:

- tietoturvaohjeen hyväksyminen ja käyttöönotto, luottamussuhteet keskeisimpien tiedonvaihdon osapuolien välillä
- tietoturvamenetelmien (ohjelmistot) toimivuus
- henkilöstön nimeäminen, tarkastaminen ja perehdyttäminen (tehdään ensimmäisessä työpajassa).

Hankepäällikkö raportoi edellytysten täyttymisestä ohjausryhmälle ensimmäisessä varsinaisessa kokouksessa.

## 3.5 Hankkeen työskentely

Hankkeen työskentelyn aikana hankepäällikkö valvoo jatkuvasti tietoturvan toteutumista, erityisesti asiakirjojen tietoturvaluokkien merkintöjä. Riskienhallinta päivitetään vähintään kuukausittain ja esitellään vakiomenettelynä ohjausryhmän kokouksissa. Erityinen huomio kiinnitetään riskien pienentämisen toimenpiteisiin ja niiden tehoon.

Tarpeen mukaan hankepäällikkö voi tehdä tarkastuksia työskentelytiloissa ja tarkastaa työskentelyyn tarvittavien välineiden tietoturvaominaisuuksia.

Tietoturvaloukkausten tapahtuessa hankepäällikkö johtaa hankkeessa vaikutusten rajoittamista, tilanteesta toipumista ja tutkintaa sikäli, kun tehtävä ei kuulu jollekin hankkeeseen osallistuvalle organisaatiolle. Työn mahdollisimman nopea jatkaminen on hankkeen tavoite.

Virheisiin puututaan välittömästi ja tarvittaessa perehdyttäminen toistetaan. Hankepäällikkö vastaa myös muutosten toteuttamisesta henkilöstön mahdollisesti vaihtuessa.

## 3.6 Hankkeen valmistuminen

Hankkeen valmistuessa hankepäällikkö varmistaa, että kaikkiin materiaaleihin on tehty tietoturvaluokkaa koskevat merkinnät ja materiaalit on luovutettu oikeassa muodossa työn tilaajalle. Hankepäällikkö varmistaa myös, että lähde- ja työmateriaalien hallinta tunnetaan ja kattava materiaalien pois kerääminen tai hävittäminen on mahdollista.

## 3.7 Hankkeen lopettaminen

Hankkeen lopettamisvaiheessa kaikki lähde- ja työmateriaalit luovutetaan hankkeen tilaajalle tai hävitetään. Hävittämisessä noudatetaan kunkin hankkeeseen osallistuvan organisaation tietoturvamateriaalien hävittämistä koskevaa ohjeistusta ja hävittäminen tehdään luotettavalla tavalla. Kaikki tietoturvaluokkaa ”käyttörajoitettu” korkeampi materiaali palautetaan hankepäällikölle. Materiaalien hävittäminen raportoidaan hankepäällikölle sähköpostitse (lyhyesti: Hankkeen käyttöön saatu ja tuotettu lähde- ja työmateriaali on hävitetty ohjeen mukaisesti ja tuotokset on palautettu hankepäällikölle).

Hankepäällikkö luovuttaa säilytettävän materiaalin muille organisaatioille tai hankkeen seuraavaan vaiheeseen. Luovuttaminen kirjataan valmistelu- tai ohjausryhmän pöytäkirjaan. Hankepäällikkö toteaa myös tietoturvavastuiden mahdollisen jatkumisen ja tiedottaa tästä asianomaisille.

Hankkeessa syntyneet kokemukset ja havainnot kerätään hankkeen tietoturvakäsikirjaksi.

# 4 Tiivistetyt tietoturvaohjeet hankkeeseen osallistujille

Nämä ovat tiivistetyt ohjeet IT-hankkeessa työskentelevälle henkilölle.

1. Perehdy hankkeen ohjeisiin ja erityisesti hankkeen tietoturvaohjeeseen
2. Vastaat omalta osaltasi tietoturvallisuuden noudattamisesta
3. Puutu virheisiin, esitä parannuksia
4. Toimi tietoturvaloukkauksessa oman organisaatiosi ohjeiden mukaisesti
5. Hankkeen tietoturva korkeintaan luokkaan ”käyttörajoitettu”, korkeammissa erillinen menettely
6. Tee NDA, selvitä turvallisuusselvityksesi tilanne
7. Käsittele hankkeen tietoja vain asianmukaisissa tiloissa ja hankkeen henkilöstön kanssa
8. Luokittele tuottamasi dokumentit
9. Merkitse luokka dokumenttiin tiedostoon, tiedostonimeen ja irrotettavaan muistivälineeseen (cd-levy)
10. Kuljeta ja säilytä materiaalia salattuna, valvottuna tai lukitussa paikassa
11. Huolehdi käyttäjätunnuksista ja salasanoista
12. Varmuuskopioi materiaali, huolehdi varmuuskopion turvallisuudesta
13. Käytä vain sallittuja ohjelmistoja ja tiedostomuotoja sekä vakioitua ja ylläpidettyä tietokonetta
14. Salaa sähköpostin liitetiedostot, muista muokata tiedostotarkenne
15. Hankkeen päättyessä luovuta ja hävitä materiaalit turvamenettelyn mukaisesti - raportoi

## Liite 3

Viite: Laki viranomaisten toiminnan julkisuudesta (621/1999) 23 §, 24 §, 35 §
Laki työelämän tietosuojasta (759/2004)

# MALLI VAITIOLOSITOUMUKSESTA

Tämä sitoumus koskee kaikkia _____ hankkeessa käyttöön saatuja käyttöoikeuksia ja tietoja. Allekirjoittaessaan tämän sitoumuksen käyttäjä sitoutuu noudattamaan seuraavia ehtoja:

1. Käyttäjä noudattaa hankkeen tietoturvaohjetta.
2. Käyttäjä käyttää hankkeen tietoja ja palveluja vain niihin tarkoituksiin ja siinä laajuudessa kuin hankkeen tietoturvaohjeen mukaan ne on tarkoitettu.
3. Käyttäjä ei paljasta mitään hankkeen tietoja sivullisille eikä käytä tietoja mihinkään hankkeen tehtävään kuulumattomiin tarkoituksiin.
4. Käyttäjä ei kopioi eikä tallenna tietoja, ellei asiasta ole erikseen sovittu hankkeen johdon kanssa. Poikkeuksena tästä ovat sähköpostiohjelmat, jotka tallettavat viestit järjestelmän ulkopuolelle. Tällöin käyttäjän tulee huolehtia viestien riittävästä suojaamisesta.
5. Käyttäjä ymmärtää, että hankejohto voi valvoa lain sallimalla tavalla työryhmäohjelmiston käyttöä tallentamalla yksityiskohtaisia tapahtumalokeja, sekä muin tarpeellisin keinoin, ja että työryhmäohjelmistojen tai niiden sisältämien tietojen käyttö tämän sitoumuksen vastaisesti voi olla rangaistavaa rikoslaissa tarkoitettuna luvattomana käyttönä, salassapitorikoksena tai muuna sellaisena rikoksena, jonka teonkuvauksen kyseinen toiminta täyttää.
6. Tässä sitoumuksessa mainituissa asioissa puhevaltaa voi käyttää vain hankkeen tietoturvasta vastaavaksi nimetty henkilö, hankkeen johtaja tai hankkeen omistajaksi määritetty henkilö.

Yllä olevan tekstin olen lukenut ja vakuutan toimivani sen mukaisesti.

Helsingissä __ . _____kuuta 20___

Vakuutuksen antaja

_____
allekirjoitus

nimen selvennys: _____

Liite: Perusmuotoinen turvallisuusselvitys (poliisilomake)

## Liite 4

# Valtiovarainministeriön voimassaolevat VAHTI-julkaisut

Hankkeen tietoturvaohje, VAHTI 9/2008

Valtionhallinnon tietoturvasanasto, VAHTI 8/2008

Informationssäkerhetsanvisning för personalen, VAHTI 7/2008

Tietoturvallisuus on asenne! Selvitys julkishallinnon tietoturvakoulutustarpeista, VAHTI 6/2008

Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys, VAHTI 5/2008

Valtionhallinnon tietoturva-arviointipoolin toimintaraportti, VAHTI 4/2008

Valtionhallinnon salauskäytäntöjen tietoturvaohje, VAHTI 3/2008

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008

VAHTIn toimintakertomus vuodelta 2007, VAHTI 1/2008

Tietoturvallisuudella tuloksia – valtionhallinnon tietoturvallisuuden yleisohje, VAHTI 3/2007

Äypuhelimien tietoturvallisuus – hyvät käytännöt, VAHTI 2/2007

Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Tietoturvakouluttajan opas, VAHTI 11/2006

Henkilöstön tietoturvaohje, VAHTI 10/2006

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006

Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006

Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006

Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006

Electronic Mail-handling Instructions for State Government, VAHTI 2/2006

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

Information Security and management by Results, VAHTI 1/2005

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004

Datasäkerhet och resultatstyrning, VAHTI 4/2004

Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004

Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004

Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003

Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003

Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003

Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003

Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002

Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002

Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002

Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001

Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000

Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin (09) 160 01
Telefaksi (09) 160 33123
www.vm.fi

9/2008
VAHTI
joulukuu 2008

ISSN 1455-2566
ISBN 978-951-804-895-7 (nid.)
ISBN 978-951-804-896-4 (pdf)